UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,820	12/08/2003	Mao Masuhiro	8008-1048	9238

466 7590 02/18/2009
YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
SCIACCA, SCOTT M	
ART UNIT	PAPER NUMBER
2446	

MAIL DATE	DELIVERY MODE
02/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/728,820
Filing Date: December 08, 2003
Appellant(s): MASUHIRO ET AL.

Thomas W. Perkins (Reg. No. 33,027)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 12/09/2008 appealing from the Office action mailed 04/11/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

GB 2 360 107 A	Moriconi et al.	9-2001
US 7,117,529	O'Donnell et al.	10-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-44 and 49-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over GB 2 360 107 A (hereinafter '107) in view of O'Donnell et al. (US 7,117,529).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-44 and 49-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over GB 2 360 107 A (hereinafter '107) in view of O'Donnell et al. (US 7,117,529).

Regarding Claim 1, '107 teaches a user authentication apparatus in a client/server type distribution system having a plurality of client devices connected to a server device over a network (See Fig. 1; *"One client 116 is shown, but server 112 is typically connected to many clients 116"* – See p. 10, lines 18-19), said server device having:

a request receiving section which receives from a server-side console a user authentication information setting request (*"policy manager 210 preferably includes a management station program 212 to operate policy manager 210"* – See p. 15, lines 3-4; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29) including user authentication information (*"A policy may contain thousands of 'security rules' that describe several constraints, including what applications a particular user can access"* – See p. 11, lines 7-8) and designation of said client devices (*"an application guard located on the client, the application guard acting to grant or deny access to various components of the client, as specified by the policy"* – See p. 10, lines 14-15; *"An optimizer program 436 within distributor 214 determines which application guard 310 needs to receive which policy rules"* – See p. 16, lines 26-28) and a nullification-of-user-authentication-information-setting request including designation of said client devices (*"Add/Delete/Modify Access 1112"* – See Fig. 11); and

a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request,

received by said request receiving section, to those of said client devices which are designated over said network (*"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5),

each of said client devices having:

a user authentication section which authenticates a user at a time of using an interface (See Fig. 13 entitled "Client Access Authorization"); and

a remote request processing section which sets said user authentication information, included in said user authentication information setting request, in said user authentication section when receiving said user authentication information setting request from said server device over said network, and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network (*"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5).

'107 does not explicitly teach the interface being a *maintenance* interface. '107 apparently performs user authentication using information in the client device. Thus, '107 does not explicitly teach the authentication being based solely on said user authentication information from a server and without regard for prior authentication information in said devices. However, O'Donnell does teach a user accessing a maintenance interface (*"An identification and authentication scheme maintains control relationships among identities in order to allow a user to dynamically grant or deny permission for a technical support representative to access the user's data"* – See

Abstract; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information). Furthermore, O'Donnell teaches user authentication being performed using information in an authentication server and NOT by a client device (*"authentication server 107 provides functionality for authenticating users for access to application server 106 and to data stored on data server 112"* – See Col. 4, lines 65-67 & Col. 5, line 1; Fig. 3 is a diagram of the authentication server. The server contains user authentication information such as Identity objects 301, Access level control module 105 and Password management 303. This information is described in detail in Col. 7, lines 11-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to specify user authentication settings for users who access a network in order to perform maintenance. Motivation for doing so would be to provide a mechanism by which a support representative may be allowed access to the network or a specific user's data without requiring the user to provide his or her personal password to the support representative (See O'Donnell, Col. 3, lines 8-13). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate a user based on user authentication information from a server device. Motivation for doing so would be to provide added security and simplicity of maintaining the authentication data in a central location.

Regarding Claim 2, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, '107 teaches setting of said user authentication information in said user authentication section in each of said

client devices being done only from the server-side console (Fig. 2 shows Management Station 212 being part of the server; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29).

Regarding Claim 3, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, '107 teaches said server device having an encryption section which encrypts said user authentication information in said user authentication information setting request to be transferred by said request transfer section, and each of said client devices having a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received by said remote request processing section (*"To secure a complex and distributed computer system, the system may typically employ a combination of encryption, authentication, and authorization technologies. Encryption is a means of sending information between participants in a manner that prevents other parties from reading the information"* – See p. 2, lines 10-13).

Regarding Claim 4, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, '107 teaches each of said client devices having a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user

authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network (*"Fig. 14 is a flowchart of method steps to evaluate authorization request"* – See p. 9, line 10; *"In order to evaluate an authorization request at application guard 310, in step 1420, evaluator 516 first searches any deny rules in local policy 318"* – See p. 21, lines 23-25; *"If, at step 1416, the evaluation finds presently valid constraints on the deny rules, then at step 1418 access is denied"* – See p. 21, lines 27-28).

Regarding Claim 5, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, O'Donnell teaches each of said client devices having a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 6, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 5. Additionally, O'Donnell teaches

each of said client devices having a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 7, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 6. Additionally, O'Donnell teaches wherein at a time a first log-in request is issued since opening of said maintenance interface, said use time extending section determines whether or not a remaining use time managed by said use time management section lies within a predetermined given time and extends said remaining use time of said use time management section by a predetermined extension time when said remaining use time lies within said predetermined given time (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 8, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 6. Additionally, O'Donnell teaches wherein during first log-in since opening of said maintenance interface, said use time extending section determines whether or not a remaining use time managed by said use time management section has fallen within a predetermined given time and extends said remaining use time of said use time management section by a predetermined

extension time when said remaining use time has fallen within said predetermined given time (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 9, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 5. Additionally, O'Donnell teaches said use time management section using, as said allowable use time, an allowable use time designated in said user authentication information setting request sent from said server device (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information).

Regarding Claim 10, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 5. Additionally, O'Donnell teaches said use time management section using an allowable use time reference value prestored in said client devices as said allowable use time (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the*

temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)" – See Col. 10, lines 4-9).

Regarding Claim 11, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 5. Additionally, O'Donnell teaches when an allowable use time is designated in said user authentication information setting request sent from said server device, said use time management section uses said designated allowable use time as said allowable use time, and when said allowable use time is not designated, said use time management section uses an allowable use time reference value prestored in said client devices as said allowable use time (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 12, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, O'Donnell teaches each of said client devices having a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section (*"At some point, the*

support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)" – See Col. 10, lines 4-13).

Regarding Claim 13, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 9. Additionally, O'Donnell teaches said log-in number management section using, as said allowable number of log-in events, an allowable number of log-in events designated in said user authentication information setting request sent from said server device (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information).

Regarding Claim 14, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 13. Additionally, O'Donnell teaches said log-in number management section using an allowable-number-of-log-in reference value prestored in said client devices as said allowable number of log-in events (*"At some point, the support representative's temporary login expires 206. Expiry can take*

place when any of the following events occur:…after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)" – See Col. 10, lines 4-13).

Regarding Claim 15, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 13. Additionally, O'Donnell teaches wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said log-in number management section uses said designated allowable number of log-in events as said allowable number of log-in events, and when said allowable number of log-in events is not designated, said log-in number management section uses an allowable-number-of-log-in reference value prestored in said client devices as said allowable number of log-in events (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:…after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 16, '107 in view of O'Donnell teaches the maintenance interface user authentication apparatus according to Claim 1. Additionally, O'Donnell teaches each of said client devices having an authentication nullification section which nullifies

said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface (*"Expiry of the temporary login ensures that, once the troubleshooting task has been completed, user data 111 remains secure"* – See Col. 10, lines 20-22).

Regarding Claim 17, '107 teaches an interface user authentication method in a client/server type distribution system comprising:

(a) a step in which a server device receives a user authentication information setting request (*"policy manager 210 preferably includes a management station program 212 to operate policy manager 210"* – See p. 15, lines 3-4; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29) including user authentication information (*"A policy may contain thousands of 'security rules' that describe several constraints, including what applications a particular user can access"* – See p. 11, lines 7-8) and designation of client devices from a server-side console and transfers said user authentication information setting request to said designated client devices over a network (*"an application guard located on the client, the application guard acting to grant or deny access to various components of the client, as specified by the policy"* – See p. 10, lines 14-15; *"An optimizer program 436 within distributor 214 determines which application guard 310 needs to receive which policy rules"* – See p. 16, lines 26-28);

(b) a step in which said client devices receive said user authentication information setting request over said network and set said user authentication information setting request in a user authentication section which authenticates a user at a time of using a maintenance interface (*"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5);

(c) a step in which said server device receives a nullification-of-user-authentication-information-setting request (*"Add/Delete/Modify Access 1112"* – See Fig. 11) including designation of said client devices from said server-side console and transfers said nullification-of-user-authentication-information-setting request to said designated client devices over said network (*"an application guard located on the client, the application guard acting to grant or deny access to various components of the client, as specified by the policy"* – See p. 10, lines 14-15; *"An optimizer program 436 within distributor 214 determines which application guard 310 needs to receive which policy rules"* – See p. 16, lines 26-28); and

(d) a step in which said client devices receive said nullification-of-user-authentication-information-setting request over said network and nullify said user authentication information set in said user authentication section (*"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5).

'107 does not explicitly teach the interface being a *maintenance* interface. '107 apparently performs user authentication using information in the client device. Thus, '107 does not explicitly teach the authentication being based solely on said user authentication information from a server and without regard for prior authentication

information in said devices. However, O'Donnell does teach a maintenance interface user authentication system (*"An identification and authentication scheme maintains control relationships among identities in order to allow a user to dynamically grant or deny permission for a technical support representative to access the user's data"* – See Abstract; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information). Furthermore, O'Donnell teaches user authentication being performed using information in an authentication server and NOT by a client device (*"authentication server 107 provides functionality for authenticating users for access to application server 106 and to data stored on data server 112"* – See Col. 4, lines 65-67 & Col. 5, line 1; Fig. 3 is a diagram of the authentication server. The server contains user authentication information such as Identity objects 301, Access level control module 105 and Password management 303. This information is described in detail in Col. 7, lines 11-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to specify user authentication settings for users who access a network in order to perform maintenance. Motivation for doing so would be to provide a mechanism by which a support representative may be allowed access to the network or a specific user's data without requiring the user to provide his or her personal password to the support representative (See O'Donnell, Col. 3, lines 8-13). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate a user based on user authentication information from a server device. Motivation for doing so would be to provide added security and simplicity of maintaining the authentication data in a central location.

Regarding Claim 18, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, '107 teaches setting of said user authentication information in said user authentication section in each of said client devices being done only from said server-side console (Fig. 2 shows Management Station 212 being part of the server; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29).

Regarding Claim 19, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, '107 teaches said step (a) including a process of causing said server device to encrypt said user authentication information to be transferred and said step (b) including a process of causing said client devices to decrypt said received user authentication information (*"To secure a complex and distributed computer system, the system may typically employ a combination of encryption, authentication, and authorization technologies. Encryption is a means of sending information between participants in a manner that prevents other parties from reading the information"* – See p. 2, lines 10-13).

Regarding Claim 20, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, '107 teaches said step (b) including a process of forcibly disabling use of a user who is currently using said

maintenance interface in case where that user authentication information which is already set in said user authentication section is set again to new user authentication information received (*"Fig. 14 is a flowchart of method steps to evaluate authorization request"* – See p. 9, line 10; *"In order to evaluate an authorization request at application guard 310, in step 1420, evaluator 516 first searches any deny rules in local policy 318"* – See p. 21, lines 23-25; *"If, at step 1416, the evaluation finds presently valid constraints on the deny rules, then at step 1418 access is denied"* – See p. 21, lines 27-28).

Regarding Claim 21, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, O'Donnell teaches the method further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 22, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 21. Additionally, O'Donnell teaches the method further including:

(f) a step in which said each of said client devices extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 23, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 22. Additionally, O'Donnell teaches the method wherein at a time a first log-in request is issued since opening of said maintenance interface, said step (f) determines whether or not a remaining use time managed in said step (e) lies within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time lies within said predetermined given time (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 24, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 22. Additionally, O'Donnell teaches the method wherein during first log-in since opening of said maintenance interface, said

step (f) determines whether or not a remaining use time managed in said step (e) has fallen within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time has fallen within said predetermined given time (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 25, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 21. Additionally, O'Donnell teaches the method wherein as said allowable use time in said step (e), an allowable use time designated in said user authentication information setting request sent from said server device is used (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information).

Regarding Claim 26, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 21. Additionally, O'Donnell teaches the method wherein as said allowable use time in said step (e), an allowable use time reference value prestored in said client devices is used (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the*

following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)" – See Col. 10, lines 4-9).

Regarding Claim 27, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 21. Additionally, O'Donnell teaches the method wherein when an allowable use time is designated in said user authentication information setting request sent from said server device, said designated allowable use time is used as said allowable use time in said step (e), and when said allowable use time is not designated, an allowable use time reference value prestored in said client devices is used as said allowable use time (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 28, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, O'Donnell teaches the method further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in

events has taken place since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 29, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 28. Additionally, O'Donnell teaches the method wherein as said allowable number of log-in events in said step (e), an allowable number of log-in events designated in said user authentication information setting request sent from said server device is used (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information).

Regarding Claim 30, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 29. Additionally, O'Donnell teaches the method wherein as said allowable number of log-in events in said step (e), an

allowable-number-of-log-in reference value prestored in said client devices is used (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:…after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 31, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 29. Additionally, O'Donnell teaches the method wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said designated allowable number of log-in events is used as said allowable number of log-in events in said step (e), and when said allowable number of log-in events is not designated, an allowable-number-of-log-in reference value prestored in said client devices is used as said allowable number of log-in events (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:…after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 32, '107 in view of O'Donnell teaches the maintenance interface user authentication method according to Claim 17. Additionally, O'Donnell teaches the method further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface (*"Expiry of the temporary login ensures that, once the troubleshooting task has been completed, user data 111 remains secure"* – See Col. 10, lines 20-22).

Regarding Claim 33, '107 teaches a server device to be connected to a plurality of client devices over a network (See Fig. 1; *"One client 116 is shown, but server 112 is typically connected to many clients 116"* – See p. 10, lines 18-19), comprising:

a request receiving section which receives from a server-side console a user authentication information setting request (*"policy manager 210 preferably includes a management station program 212 to operate policy manager 210"* – See p. 15, lines 3-4; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29) including user authentication information, which is set in user authentication section for authenticating a user at a time said client devices use an interface (*"A policy may contain thousands of 'security rules' that describe several constraints, including what applications a particular user can access"* – See p. 11, lines 7-8), and designation of said client devices (*"an application guard located on the client, the application guard acting to grant or deny*

access to various components of the client, as specified by the policy" – See p. 10, lines 14-15; *"An optimizer program 436 within distributor 214 determines which application guard 310 needs to receive which policy rules"* – See p. 16, lines 26-28) and a nullification-of-user-authentication-information-setting request including designation of said client devices (*"Add/Delete/Modify Access 1112"* – See Fig. 11); and

a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request, received by said request receiving section, to those of said client devices which are designated over said network (*"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5).

'107 does not explicitly teach the interface being a *maintenance* interface. However, O'Donnell does teach client devices using a maintenance interface (*"An identification and authentication scheme maintains control relationships among identities in order to allow a user to dynamically grant or deny permission for a technical support representative to access the user's data"* – See Abstract; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information). It would have been obvious to one of ordinary skill in the art at the time the invention was made to specify user authentication settings for users who access a network in order to perform maintenance. Motivation for doing so would be to provide a mechanism by which a support representative may be allowed access to the network or a specific user's data without requiring the user to provide his or her personal password to the support representative (See O'Donnell, Col. 3, lines 8-13).

Regarding Claim 34, '107 in view of O'Donnell teaches the server device according to Claim 33. Additionally, '107 teaches an encryption section which encrypts said user authentication information in said user authentication information setting request to be transferred by said request transfer section (*"To secure a complex and distributed computer system, the system may typically employ a combination of encryption, authentication, and authorization technologies. Encryption is a means of sending information between participants in a manner that prevents other parties from reading the information"* – See p. 2, lines 10-13).

Regarding Claim 35, '107 in view of O'Donnell teaches the server device according to Claim 33. Additionally, O'Donnell teaches each of said client devices having a structure for transmitting said allowable use time to be set in use time management section, which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section, in such a way as to be included in said user authentication information setting request (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 36, '107 in view of O'Donnell teaches the server device according to Claim 33. Additionally, O'Donnell teaches each of said client devices having a structure for transmitting said allowable number of log-in events to be set in a log-in number management section, which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section, in such a way as to be included in said user authentication information setting request (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 37, '107 teaches a client device to be connected to a server device over a network (See Fig. 1), comprising:

a user authentication section which authenticates a user at a time of using an interface (See Fig. 13 entitled "Client Access Authorization"); and

a remote request processing section which sets user authentication information, included in a user authentication information setting request, in said user authentication section when receiving said user authentication information setting request (*"Server 112*

preferably contains a program stored in non-volatile memory 124 for managing a policy or a set of rules and then distributing the policy to client 116 via link 114" – See p. 10, lines 26-28) including said user authentication information from said server device over said network (*"A policy may contain thousands of 'security rules' that describe several constraints, including what applications a particular user can access"* – See p. 11, lines 7-8), and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network (*"Add/Delete/Modify Access 1112"* – See Fig. 11; *"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5).

'107 does not explicitly teach the interface being a *maintenance* interface. '107 apparently performs user authentication using information in the client device. Thus, '107 does not explicitly teach the authentication being based solely on said user authentication information from a server and without regard for prior authentication information in said devices. However, O'Donnell does teach a user accessing a maintenance interface (*"An identification and authentication scheme maintains control relationships among identities in order to allow a user to dynamically grant or deny permission for a technical support representative to access the user's data"* – See Abstract; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information). Furthermore, O'Donnell teaches user authentication being performed using information in an authentication server and NOT by a client device (*"authentication server 107 provides functionality for authenticating*

users for access to application server 106 and to data stored on data server 112" – See Col. 4, lines 65-67 & Col. 5, line 1; Fig. 3 is a diagram of the authentication server. The server contains user authentication information such as Identity objects 301, Access level control module 105 and Password management 303. This information is described in detail in Col. 7, lines 11-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to specify user authentication settings for users who access a network in order to perform maintenance. Motivation for doing so would be to provide a mechanism by which a support representative may be allowed access to the network or a specific user's data without requiring the user to provide his or her personal password to the support representative (See O'Donnell, Col. 3, lines 8-13). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate a user based on user authentication information from a server device. Motivation for doing so would be to provide added security and simplicity of maintaining the authentication data in a central location.

Regarding Claim 38, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, '107 teaches setting of said user authentication information in said user authentication section being done only by said user authentication information setting request received from said server device (Fig. 2 shows Management Station 212 being part of the server; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29).

Regarding Claim 39, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, '107 teaches the client device further comprising a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received from said server device over said network (*"To secure a complex and distributed computer system, the system may typically employ a combination of encryption, authentication, and authorization technologies. Encryption is a means of sending information between participants in a manner that prevents other parties from reading the information"* – See p. 2, lines 10-13).

Regarding Claim 40, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, '107 teaches the client device further comprising a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network (*"Fig. 14 is a flowchart of method steps to evaluate authorization request"* – See p. 9, line 10; *"In order to evaluate an authorization request at application guard 310, in step 1420, evaluator 516 first searches any deny rules in local policy 318"* – See p. 21, lines 23-25; *"If, at step 1416, the evaluation finds presently valid constraints on the deny rules, then at step 1418 access is denied"* – See p. 21, lines 27-28).

Regarding Claim 41, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, O'Donnell teaches the client device further comprising a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 42, '107 in view of O'Donnell teaches the client device according to Claim 41. Additionally, O'Donnell teaches the client device further comprising a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 43, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, O'Donnell teaches the client device further

comprising a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:…after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information).

Regarding Claim 44, '107 in view of O'Donnell teaches the client device according to Claim 37. Additionally, O'Donnell teaches the client device further comprising an authentication nullification section which nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface (*"Expiry of the temporary login ensures that, once the troubleshooting task has been completed, user data 111 remains secure"* – See Col. 10, lines 20-22).

Regarding Claim 49, '107 teaches a client program stored in a computer-readable medium and comprising computer-executable instructions for causing a

computer constituting a client device to be connected to a server device over a network to function as:

a user authentication section which authenticates a user at a time of using an interface (See Fig. 13 entitled "Client Access Authorization"); and

a remote request processing section which sets user authentication information, included in a user authentication information setting request, in said user authentication section when receiving said user authentication information setting request (*"Server 112 preferably contains a program stored in non-volatile memory 124 for managing a policy or a set of rules and then distributing the policy to client 116 via link 114"* – See p. 10, lines 26-28) including said user authentication information from said server device over said network (*"A policy may contain thousands of 'security rules' that describe several constraints, including what applications a particular user can access"* – See p. 11, lines 7-8), and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network (*"Add/Delete/Modify Access 1112"* – See Fig. 11; *"a distributor program 214 to distribute local client policies to clients"* – See p. 15, lines 4-5).

'107 does not explicitly teach the interface being a *maintenance* interface. '107 apparently performs user authentication using information in the client device. Thus, '107 does not explicitly teach the authentication being based solely on said user authentication information from a server and without regard for prior authentication information in said devices. However, O'Donnell does teach a user accessing a

maintenance interface (*"An identification and authentication scheme maintains control relationships among identities in order to allow a user to dynamically grant or deny permission for a technical support representative to access the user's data"* – See Abstract; In the context of O'Donnell's disclosure, the user is the one who controls access and authentication information). Furthermore, O'Donnell teaches user authentication being performed using information in an authentication server and NOT by a client device (*"authentication server 107 provides functionality for authenticating users for access to application server 106 and to data stored on data server 112"* – See Col. 4, lines 65-67 & Col. 5, line 1; Fig. 3 is a diagram of the authentication server. The server contains user authentication information such as Identity objects 301, Access level control module 105 and Password management 303. This information is described in detail in Col. 7, lines 11-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to specify user authentication settings for users who access a network in order to perform maintenance. Motivation for doing so would be to provide a mechanism by which a support representative may be allowed access to the network or a specific user's data without requiring the user to provide his or her personal password to the support representative (See O'Donnell, Col. 3, lines 8-13). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate a user based on user authentication information from a server device. Motivation for doing so would be to provide added security and simplicity of maintaining the authentication data in a central location.

Regarding Claim 50, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, '107 teaches setting of said user authentication information in said user authentication section being done only by said user authentication information setting request received from said server device (Fig. 2 shows Management Station 212 being part of the server; *"management station 212 preferably includes a graphical user interface (GUI) 410 for creating or customizing rules by system users"* – See p. 15, lines 28-29).

Regarding Claim 51, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, '107 teaches said computer being further caused to function as a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received from said server device over said network (*"To secure a complex and distributed computer system, the system may typically employ a combination of encryption, authentication, and authorization technologies. Encryption is a means of sending information between participants in a manner that prevents other parties from reading the information"* – See p. 2, lines 10-13).

Regarding Claim 52, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, '107 teaches said computer being further caused to function as a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication

information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network (*"Fig. 14 is a flowchart of method steps to evaluate authorization request"* – See p. 9, line 10; *"In order to evaluate an authorization request at application guard 310, in step 1420, evaluator 516 first searches any deny rules in local policy 318"* – See p. 21, lines 23-25; *"If, at step 1416, the evaluation finds presently valid constraints on the deny rules, then at step 1418 access is denied"* – See p. 21, lines 27-28).

Regarding Claim 53, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, O'Donnell teaches said computer being further caused to function as a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur: after a predetermined time period has elapsed (e.g. the temporary login may only last 24 hours, or some other time period that is preset or selectable by the user)"* – See Col. 10, lines 4-9).

Regarding Claim 54, '107 in view of O'Donnell teaches the client program according to Claim 53. Additionally, O'Donnell teaches said computer being further

caused to function as a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface (*"The user may also retain the ability to terminate (or extend) the representative's access privileges at any time"* – See Col. 3, lines 25-27).

Regarding Claim 55, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, O'Donnell teaches said computer being further caused to function as a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who Is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information In said user authentication section (*"At some point, the support representative's temporary login expires 206. Expiry can take place when any of the following events occur:...after a predetermined number of uses of the temporary login (e.g. the temporary login may expire after three uses, or some other number of uses, the number being preset or selectable by the user)"* – See Col. 10, lines 4-13).

Regarding Claim 56, '107 in view of O'Donnell teaches the client program according to Claim 49. Additionally, O'Donnell teaches said computer being further caused to function as an authentication nullification section which nullifies said user authentication information set in said user authentication section at a time a user of said

maintenance interface ends use of said maintenance interface (*"Expiry of the temporary login ensures that, once the troubleshooting task has been completed, user data 111 remains secure"* – See Col. 10, lines 20-22).

(10) Response to Argument

The examiner summarizes the various points raised by the appellant and addresses them individually.

(A) Appellant Argues: "These claims provide, among other features, that authentication is based solely on the user authentication information from the server device and without regard for prior authentication information in the client device. As explained below, the references do not disclose or suggest that authentication when opening a maintenance interface in the client device is to be based solely on the input from the server without regard for prior authentication information. In the prior art, the authentication is predicated on permission from a client device, not based solely on the user authentication information from the server (e.g., GB'107 Figure 13, element 1310 and page 21, lines 9-21; and O'DONNELL et al. column 8, lines 15-62).

GB'107 describes a framework by which security policy and application guards are distributed from a policy manager located in a server. The reference does not disclose that permission to open a maintenance interface at a client device can be carried out from a maintenance console of a server. In GB'107 a series of actions are commenced by a permission request from a client device. By contrast, in the present

invention, actuation of a maintenance console at a client device is enabled by permission given from the maintenance console of a server regardless of the permission request from the client device.

O'DONNELL et al. describe a system in which a client device (user) is able to dynamically grant or deny permission for a technical support representative to access the user's data. That is, authorization depends on access granted by the user, not solely on user authentication information from the server. Note, for example, that in column 8 O'DONNELL et al. refer to the user specifying data to which the support representative is authorized to access. The support representative is authorized access to the client device and cannot connect to the client device without access from the client-side console. There is nothing in the reference that suggests that authentication is to be based solely on the user authentication information from the server device and without regard for prior authentication information in the client device. Indeed, O'DONNELL et al. predicate authorization on actions by the client device (e.g., column 8, lines 49-53)."

In Response: Examiner would first like to point out that the material that Appellant pointed out from GB'107 (Figure 13, element 130 and page 21, lines 9-21) is irrelevant since nothing from this reference was relied upon with respect to the claimed feature of authenticating "based solely on said user authentication information from said server device".

In the Office action mailed on 04/11/2008, Examiner relied on O'Donnell to disclose the feature where user authentication is "based solely on said user authentication information from said server device and without regard for prior authentication information in said client devices". However, Appellant argues that O'Donnell discloses authentication being predicated on permission from a client device and not based solely on user authentication information from the server. As evidence of this, Appellant points to Col. 8 of O'Donnell. The portions of Col. 8 which have been cited by the Appellant deal with *authorization* of a user. The portions of O'Donnell that were cited by the Examiner in the 103(a) rejection deal with *authentication*, which is consistent with the language in the claimed invention.

There is an important distinction that needs to be made between *authorization* and *authentication*. Authorization deals with assigning permissions. In the case of O'Donnell's disclosure, varying authorization levels are assigned to support representatives. In contrast, authentication deals with establishing the validity or genuineness of something. O'Donnell performs authentication by maintaining authentication information in an authentication server 107 (See Fig. 3) and using the information to verify the credentials of a support representative (See Col. 8, lines 4-6 & Col. 8, lines 59-62). Thus, as far as *authentication* is concerned, O'Donnell only discloses authentication being performed based on information in a server and says nothing about authentication being based on prior authentication information from client devices.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Scott M. Sciacca/

Examiner, Art Unit 2446

12 February 2009

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451

Conferees:

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451